DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD National Industrial Security Program Operating Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING
a. FACILITY CLEARANCE REQUIRED: **TOP SECRET**
b. LEVEL OF SAFEGUARDING REQUIRED: **SECRET**

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)			3. THIS SPECIFICATION IS: (X and complete as applicable)			
	a. PRIME CONTRACT NUMBER		X	a. ORIGINAL (Complete date in all cases)		DATE (YYYYMMDD) 20030131
	b. SUBCONTRACT NUMBER			b. REVISED (Supersedes all previous specs)	Revision Number	DATE (YYYYMMDD)
X	c. SOLICITATION OR OTHER NUMBER N00421-03-R-TBD	DUE DATE (YYYYMMDD)		c. FINAL (Complete item 5 in all cases)		DATE (YYYYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If YES, complete the following: N00421-97-C-1105
Classified material received or generated under _____ (preceding contract number) is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If YES, complete the following:
In response to the contractor's request dated _____ retention of the identified classified material is authorized for the period of _____.

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
FOR BIDDING PURPOSES ONLY – NOT VALID FOR ACTUAL CONTRACT		

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT
Engineering and technical services in support of non-cooperative target recognition, non-cooperative target identification, and other combat identification and air traffic control systems.
COR: Greg Penk, 301-995-8212, ACOR: Chris Utara, 301-995-8195

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FORMERLY RESTRICTED DATA		X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY		X
(1) SENSITIVE COMPARTMENT INFORMATION (SCI)		X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	X	
(2) NON-SCI	X		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X
f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT		X
g. NATO INFORMATION	X		i. HAVE TEMPEST REQUIREMENTS		X
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS 2/4/03	X	
i. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER (Specify)		X
k. OTHER (Specify)					

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except a provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. government authority. Proposed public releases shall be submitted for approval prior to release

[ ] Direct [X] Through (Specify):

COMMANDING OFFICER, NAWCAD/NAS PAO 301.342.7710
UNIT NASAD, BLDG 409
22268 CEDAR POINT ROAD
PATUXENT RIVER, MARYLAND 20670-1154

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Security of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

The majority of performance will be at Webster Field in buildings 8104, 8124, 8141, 8164, and 8220 and includes training of U.S. and foreign personnel on radar systems. Classified portions will be for U.S. personnel only.

10e.(2) Contract requires access to the SIPRNET. Although intelligence data is available on SIPRNET, and could be inadvertently accessed, there is no valid requirement for intelligence at this time. Therefore, contractor shall not intentionally access or download intelligence data from the SIPRNET. In the event, intelligence data is required, the COR or TPOC will modify this requirement for submission to the NAVAIR/NAWCAD STILO. Written approval of the User Agency Contracting Officer is required prior to subcontracting.

Reviewed by: _____
(Senior Intelligence Officer: Stephen Hendricks

10g. A final U.S. Government clearance, at the appropriate level, is required for access to NATO information. Written approval of the Contracting Officer is required prior to subcontracting.

Contractor will have access to and be custodians on U.S. Gov't security containers in building 8164 at Webster Field.

10j. For Official Use Only information generated and/or provided under this contract shall be marked and safeguarded as specified in DoD 5400.7-R, Chapters 3 and 4 (attached).

11c. Classification markings in the material to be furnished will provide the classification guidance necessary for performance. Applicable classification guides: DoD International AIMS Program Security Classification Guide, dated 31 March 1997; Radar Track Discriminator System Classification Guide (enclosure 117 to OPNAVINST S5513.3B) will be given to contractor on contract award. If further guidance is required contact the TPOC/COR listed in block 9. Further guidance will be provided by the Government on site and at each site being visited.

The contractor shall comply with the requirements of the Information Systems Security Programs as described in NAVAIRWARCENACDIVINST 5239.1. All systems, regardless of the level of data processed, will be accredited in accordance with the above instructions. [Contracts will provide copies of these instructions.]

11f. Limited performance will be at overseas locations aboard U.S. ships and installations only. Access to U.S. classified information will be aboard U.S. ships and installations only. Possible location include Yokosuka, Japan; Sasebo, Japan; Naples, Italy; Okinawa, Japan; Rota, Spain; and Diego Garcia, Indian Ocean.

11j. The contractor shall develop, implement and maintain a facility level OPSEC program to protect classified and sensitive unclassified information to be used at the contractor facility during the performance of this contract. contract data requirements list (CDRL) and data item description (DID) attached. The OPSEC plan shall be submitted to NAWCAD 7.4.3 within 90 days of contract award for acceptance and approval. Contractor shall mail draft OPSEC Plan to Commander, Att: 7.4.3, B463, UNIT 10, 22514 Mccoy Road, Patuxent River, MD 20670-1457. While performing aboard NAWCAD sites, the contractor shall comply with the provisions of NAWCADINST 3432.1A at all other sites, the contractor shall comply with the local command and/or program OPSEC plan.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to NISPOM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 if additional space is needed.) [X] YES [ ] NO

SEE BLOCK 13

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.) [ ] YES [X] NO

NONE

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
JOYCE K. FOCA	CONTRACTING OFFICER'S SECURITY REPRESENTATIVE (COSR)	(301)757-6580

d. ADDRESS (Include Zip Code)	17. REQUIRED DISTRIBUTION	
COMMANDER, 7.4.1 BLDG 463, R102, 22514 McCOY ROAD NAVAL AIR WARFARE CENTER AIRCRAFT DIVISION PATUXENT RIVER, MD 20670-1161	X	a. CONTRACTOR
		b. SUBCONTRACTOR
	X	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
		d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
		e. ADMINISTRATIVE CONTRACTING OFFICER
e. SIGNATURE Barbara J. Jenwik 2/5/03	X	f. OTHERS AS NECESSARY COR, COSR

Attachment G

DD Form 254 DEC 99

C3. CHAPTER 3

EXEMPTIONS

C3.1. GENERAL PROVISIONS

C3.1.1. General. Records that meet the exemption criteria of the FOIA may be withheld from public disclosure and need not be published in the Federal Register, made available in a library reading room, or provided in response to a FOIA request.

C3.2. EXEMPTIONS

C3.2.1. FOIA Exemptions. The following types of records may be withheld in whole or in part from public disclosure under the FOIA, unless otherwise prescribed by law: A discretionary release of a record (see also subsection C1.5.5., above) to one requester shall prevent the withholding of the same record under a FOIA exemption if the record is subsequently requested by someone else. However, a FOIA exemption may be invoked to withhold information that is similar or related that has been the subject of a discretionary release. In applying exemptions, the identity of the requester and the purpose for which the record is sought are irrelevant with the exception that an exemption may not be invoked where the particular interest to be protected is the requester's interest. *However, if the subject of the record is the requester for the record and the record is contained in a Privacy Act system of records, it may only be denied to the requester if withholding is both authorized by DoD 5400.11-R (reference (v)) and by a FOIA exemption.*

C3.2.1.1. Number 1. (5 U.S.C. 552 (b)(1)) (reference (a)). Those properly and currently classified in the interest of national defense or foreign policy, as specifically authorized under the criteria established by Executive Order and implemented by regulations, such as DoD 5200.1-R (reference (g)). Although material is not classified at the time of the FOIA request, a classification review may be undertaken to determine whether the information should be classified. The procedures in reference (g) apply. If the information qualifies as Exemption 1 information, there is **no discretion** regarding its release. In addition, this exemption shall be invoked when the following situations are apparent:

C3.2.1.1.1. The fact of the existence or nonexistence of a record would itself reveal classified information. In this situation, Components shall neither confirm nor deny the existence or nonexistence of the record being requested. A

"refusal to confirm or deny" response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no record" response when a record does not exist, and a "refusal to confirm or deny" when a record does exist will itself disclose national security information.

C3.2.1.1.2. Compilations of items of information that are individually unclassified may be classified if the compiled information reveals additional association or relationship that meets the standard for classification under an existing executive order for classification and DoD 5200.1-R (reference (g)), and is not otherwise revealed in the individual items of information.

C3.2.1.2. Number 2. (5 U.S.C. 552 (b)(2)) (reference (a)). Those related solely to the internal personnel rules and practices of the Department of Defense or any of its Components. This exemption is **entirely discretionary.** This exemption has two profiles, **high (b)(2) and low (b)(2).** Paragraph C3.2.1.2.2., below, contains a brief discussion on the low (b)(2) profile; however, that discussion is for information purposes only. When only a minimum Government interest would be affected (administrative burden), there is a great potential for discretionary disclosure of the information. Consequently, DoD Components **shall not invoke** the low (b)(2) profile.

C3.2.1.2.1. Records qualifying under high (b)(2) are those containing or constituting statutes, rules, regulations, orders, manuals, directives, instructions, and security classification guides, the release of which would allow circumvention of these records thereby substantially hindering the effective performance of a significant function of the Department of Defense. Examples include:

C3.2.1.2.1.1. Those operating rules, guidelines, and manuals for DoD investigators, inspectors, auditors, or examiners that must remain privileged in order for the DoD Component to fulfill a legal requirement.

C3.2.1.2.1.2. Personnel and other administrative matters, such as examination questions and answers used in training courses or in the determination of the qualifications of candidates for employment, entrance on duty, advancement, or promotion.

C3.2.1.2.1.3. Computer software, the release of which would allow circumvention of a statute or DoD rules, Regulations, orders, Manuals, Directives, or Instructions. In this situation, the **use** of the software must be closely examined to ensure a circumvention possibility exists.

C3.2.1.2.2. Records qualifying under the low (b)(2) profile are those that are trivial and housekeeping in nature for which there is no legitimate public interest or benefit to be gained by release, and it would constitute an administrative burden to process the request in order to disclose the records. Examples include rules of personnel's use of parking facilities or regulation of lunch hours, statements of policy as to sick leave, and administrative data such as file numbers, mail routing stamps, initials, data processing notations, brief references to previous communications, and other like administrative markings. DoD Components shall not invoke the low (b)(2) profile.

C3.2.1.3. Number 3. (5 U.S.C. 552 (b)(3)) (reference (a)). Those concerning matters that a statute specifically exempts from disclosure by terms that permit **no discretion** on the issue, or in accordance with criteria established by that statute for withholding or referring to particular types of matters to be withheld. The Directorate for Freedom of Information and Security Review maintains a list of (b)(3) statutes used within the Department of Defense, and provides updated lists of these statutes to DoD Components on a periodic basis. A few examples of such statutes are:

C3.2.1.3.1. Patent Secrecy, 35 U.S.C. 181-188 (reference (h)). Any records containing information relating to inventions that are the subject of patent applications on which Patent Secrecy Orders have been issued.

C3.2.1.3.2. Restricted Data and Formerly Restricted Data, 42 U.S.C. 2162 (reference (i)).

C3.2.1.3.3. Communication Intelligence, 18 U.S.C. 798 (reference (j)).

C3.2.1.3.4. Authority to Withhold From Public Disclosure Certain Technical Data, 10 U.S.C. 130 and DoD Directive 5230.25 (references (k) and (l)).

C3.2.1.3.5. Confidentiality of Medical Quality Assurance Records: Qualified Immunity for Participants, 10 U.S.C. 1102 f (reference (m)).

C3.2.1.3.6. Physical Protection of Special Nuclear Material: Limitation on Dissemination of Unclassified Information, 10 U.S.C. 128 (reference (n)).

C3.2.1.3.7. Protection of Intelligence Sources and Methods, 50 U.S.C. 403-3(c)(*6*) (reference (o)).

C3.2.1.3.8. Protection of Contractor Submitted Proposals, 10 U.S.C.

2305(g) (reference (p)).

C3.2.1.3.9. Procurement Integrity, 41 U.S.C. 423 (reference (q)).

C3.2.1.4. Number 4. (5 U.S.C. 552 (b)(4)) (reference (a)). Those containing trade secrets or commercial or financial information that a DoD Component receives from a person or organization outside the Government with the understanding that the information or record will be retained on a privileged or confidential basis in accordance with the customary handling of such records. Records within the exemption must contain trade secrets, or commercial or financial records, the disclosure of which is likely to cause substantial harm to the competitive position of the source providing the information; impair the Government's ability to obtain necessary information in the future; or impair some other legitimate Government interest. Commercial or financial information submitted on a voluntary basis, absent any exercised authority prescribing criteria for submission is protected without any requirement to show competitive harm (see paragraph C3.2.1.4.8., below). If the information qualifies as Exemption 4 information, there is **no discretion** in its release. Examples include:

C3.2.1.4.1. Commercial or financial information received in confidence in connection with loans, bids, contracts, or proposals set forth in or incorporated by reference in a contract entered into between the DoD Component and the offeror that submitted the proposal, as well as other information received in confidence or privileged, such as trade secrets, inventions, discoveries, or other proprietary data. See also C5.2.8.2., below, this Regulation. Additionally, when the provisions of 10 U.S.C. 2305(g) (reference (p)), and 41 U.S.C. 423 (reference (q)) are met, certain proprietary and source selection information may be withheld under Exemption 3.

C3.2.1.4.2. Statistical data and commercial or financial information concerning contract performance, income, profits, losses, and expenditures, if offered and received in confidence from a contractor or potential contractor.

C3.2.1.4.3. Personal statements given in the course of inspections, investigations, or audits, when such statements are received in confidence from the individual and retained in confidence because they reveal trade secrets or commercial or financial information normally considered confidential or privileged.

C3.2.1.4.4. Financial data provided in confidence by private employers in connection with locality wage surveys that are used to fix and adjust pay schedules applicable to the prevailing wage rate of employees within the Department of Defense.

C3.2.1.4.5. Scientific and manufacturing processes or developments concerning technical or scientific data or other information submitted with an application for a research grant, or with a report while research is in progress.

C3.2.1.4.6. Technical or scientific data developed by a contractor or subcontractor exclusively at private expense, and technical or scientific data developed in part with Federal funds and in part at private expense, wherein the contractor or subcontractor has retained legitimate proprietary interests in such data in accordance with 10 U.S.C. 2320-2321 (reference (r)) and DoD Federal Acquisition Regulation Supplement (DFARS), Chapter 2 of 48 C.F.R., Subpart 227.71-227.72 (reference (s)). Technical data developed exclusively with Federal funds may be withheld under Exemption Number 3 if it meets the criteria of 10 U.S.C. 130 (reference (k)) and DoD Directive 5230.25 (reference (l)) (see subsection C3.2.1., Number 3 C3.2.1.3.5., above).

C3.2.1.4.7. Computer software which is copyrighted under the Copyright Act of 1976 (17 U.S.C. 106) (reference (t)), the disclosure of which would have an adverse impact on the potential market value of a copyrighted work.

C3.2.1.4.8. Proprietary information submitted strictly on a **voluntary** basis, absent any exercised authority prescribing criteria for submission. Examples of exercised authorities prescribing criteria for submission are statutes, Executive Orders, regulations, invitations for bids, requests for proposals, and contracts. Submission of information under these authorities **is not voluntary**. (See also subsection C5.2.8.3., below.)

C3.2.1.5. Number 5. (5 U.S.C. 552 (b)(5)) (reference (a)). Those containing information considered privileged in litigation, primarily under the deliberative process privilege. Except as provided in paragraphs Number 5 C3.2.1.5.2. through C3.2.1.5.5., below, internal advice, recommendations, and subjective evaluations, as contrasted with factual matters, that are reflected in deliberative records pertaining to the decision-making process of an Agency, whether within or among Agencies (as defined in 5 U.S.C. 552(e) (reference (a)), or within or among DoD Components. In order to meet the test of this exemption, the record must be both deliberative in nature, as well as part of a decision-making process. Merely being an internal record is insufficient basis for withholding under this exemption. Also potentially exempted are records pertaining to the attorney-client privilege and the attorney work-product privilege. This exemption is **entirely discretionary**.

C3.2.1.5.1. Examples of the deliberative process include:

C3.2.1.5.1.1. The non-factual portions of staff papers, to include after-action reports, lessons learned, and situation reports containing staff evaluations, advice, opinions, or suggestions.

C3.2.1.5.1.2. Advice, suggestions, or evaluations prepared on behalf of the Department of Defense by individual consultants or by boards, committees, councils, groups, panels, conferences, commissions, task forces, or other similar groups that are formed for the purpose of obtaining advice and recommendations.

C3.2.1.5.1.3. Those non-factual portions of evaluations by DoD Component personnel of contractors and their products.

C3.2.1.5.1.4. Information of a speculative, tentative, or evaluative nature or such matters as proposed plans to procure, lease or otherwise acquire and dispose of materials, real estate, facilities or functions, when such information would provide undue or unfair competitive advantage to private personal interests or would impede legitimate Government functions.

C3.2.1.5.1.5. Trade secret or other confidential research development, or commercial information owned by the Government, where premature release is likely to affect the Government's negotiating position or other commercial interest.

C3.2.1.5.1.6. Those portions of official reports of inspection, reports of the Inspector Generals, audits, investigations, or surveys pertaining to safety, security, or the internal management, administration, or operation of one or more DoD Components, when these records have traditionally been treated by the courts as privileged against disclosure in litigation.

C3.2.1.5.1.7. Planning, programming, and budgetary information that is involved in the defense planning and resource allocation process.

C3.2.1.5.2. If any such intra- or inter-agency record or reasonably segregable portion of such record hypothetically would be made available routinely through the discovery process in the course of litigation with the Agency, then it should not be withheld under the FOIA. If, however, the information hypothetically would not be released at all, or would only be released in a particular case during civil

discovery where a party's particularized showing of need might override a priviledge, then the record may be withheld. Discovery is the formal process by which litigants obtain information from each other for use in the litigation. Consult with legal counsel to determine whether Exemption 5 material would be routinely made available through the discovery process.

C3.2.1.5.3. Intra- or inter-agency memoranda or letters that are factual, or those reasonably segregable portions that are factual, are routinely made available through discovery, and shall be made available to a requester, unless the factual material is otherwise exempt from release, inextricably intertwined with the exempt information, so fragmented as to be uninformative, or so redundant of information already available to the requester as to provide no new substantive information.

C3.2.1.5.4. A direction or order from a superior to a subordinate, though contained in an internal communication, generally cannot be withheld from a requester if it constitutes policy guidance or a decision, as distinguished from a discussion of preliminary matters or a request for information or advice that would compromise the decision-making process.

C3.2.1.5.5. An internal communication concerning a decision that subsequently has been made a matter of public record must be made available to a requester when the rationale for the decision is expressly adopted or incorporated by reference in the record containing the decision.

C3.2.1.6. Number 6. (5 U.S.C. 552 (b)(6)) (reference (a)). Information in personnel and medical files, as well as similar personal information in other files, that, if disclosed to a requester, other than the person about whom the information is about, would result in a clearly unwarranted invasion of personal privacy. Release of information about an individual contained in a Privacy Act System of records that would constitute a clearly unwarranted invasion of privacy is prohibited, and could subject the releaser to civil and criminal penalties. If the information qualifies as Exemption 6 information, there is **no discretion** in its release.

C3.2.1.6.1. Examples of other files containing personal information similar to that contained in personnel and medical files include:

C3.2.1.6.1.1. Those compiled to evaluate or adjudicate the suitability of candidates for civilian employment or membership in the Armed Forces, and the eligibility of individuals (civilian, military, or contractor employees) for security clearances, or for access to particularly sensitive classified information.

C3.2.1.6.1.2. Files containing reports, records, and other material pertaining to personnel matters in which administrative action, including disciplinary action, may be taken.

C3.2.1.6.2. Home addresses, *including private e-mail addresses,* are normally not releasable without the consent of the individuals concerned. This includes lists of home addressees and military quarters' addressees without the occupant's name. *Additionally, the names and duty addresses (postal and/or e-mail) of DoD military and civilian personnel who are assigned to units that are sensitive, routinely deployable, or stationed in foreign territories can constitute a clearly unwarranted invasion of personal privacy.*

C3.2.1.6.2.1. Privacy Interest. A privacy interest may exist in personal information even though the information has been disclosed at some place and time. If personal information is not freely available from sources other than the Federal Government, a privacy interest exists in its nondisclosure. The fact that the Federal Government expended funds to prepare, index and maintain records on personal information, and the fact that a requester invokes FOIA to obtain these records indicates the information is not freely available.

C3.2.1.6.2.2. Names and duty addresses *(postal and/or e-mail)* published in telephone directories, organizational charts, rosters and similar materials for personnel assigned to units that are sensitive, routinely deployable, or stationed in foreign territories are withholdable under this exemption.

C3.2.1.6.3. This exemption shall not be used in an attempt to protect the privacy of a deceased person, but it may be used to protect the privacy of the deceased person's family if disclosure would rekindle grief, anguish, pain, embarrassment, or even disruption of peace of mind of surviving family members. In such situations, balance the surviving family members' privacy against the public's right to know to determine if disclosure is in the public interest. Additionally, the deceased's social security number should be withheld since it is used by the next of kin to receive benefits. Disclosures may be made to the immediate next of kin as defined in DoD Directive 5154.24 (reference (u)).

C3.2.1.6.4. A clearly unwarranted invasion of the privacy of third parties identified in a personnel, medical or similar record constitutes a basis for deleting those reasonably segregable portions of that record. When withholding third party personal information from the subject of the record and the record is contained in

a Privacy Act system of records, consult with legal counsel.

C3.2.1.6.5. This exemption also applies when the fact of the existence or nonexistence of a responsive record would itself reveal personally private information, and the public interest in disclosure is not sufficient to outweigh the privacy interest. In this situation, DoD Components shall neither confirm nor deny the existence or nonexistence of the record being requested. This is a Glomar response, and Exemption 6 must be cited in the response. Additionally, in order to insure personal privacy is not violated during referrals, DoD Components shall coordinate with other DoD Components or Federal Agencies **before** referring a record that is exempt under the Glomar concept.

C3.2.1.6.5.1. A "refusal to confirm or deny" response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no records" response when a record does not exist and a "refusal to confirm or deny" when a record does exist will itself disclose personally private information.

C3.2.1.6.5.2. Refusal to confirm or deny should not be used when (a) the person whose personal privacy is in jeopardy has provided the requester a waiver of his or her privacy rights; (b) the person initiated or directly participated in an investigation that lead to the creation of an Agency record seeks access to that record; or (c) the person whose personal privacy is in jeopardy is deceased, the Agency is aware of that fact, and disclosure would not invade the privacy of the deceased's family. See paragraph Number C3.2.1.6.3., above.

C3.2.1.7. Number 7. (5 U.S.C. 552 (b)(7)) (reference (a)). Records or information compiled for law enforcement purposes; i.e., civil, criminal, or military law, including the implementation of Executive Orders or regulations issued pursuant to law. This exemption may be invoked to prevent disclosure of documents not originally created for, but later gathered for law enforcement purposes. **With the exception of parts (C) and (F)** (see subparagraph Number 7 C3.2.1.7.1.3., below) of this exemption, this exemption **is discretionary**. If information qualifies as exemption **(7)(C) or (7)(F)** (see subparagraph Number 7 C3.2.1.7.1.3., below) information, there is **no discretion** in its release.

C3.2.1.7.1. This exemption applies, however, only to the extent that production of such law enforcement records or information could result in the following:

C3.2.1.7.1.1. Could reasonably be expected to interfere with enforcement proceedings (5 U.S.C. 552(b)(7)(A)) (reference (a)).

C3.2.1.7.1.2. Would deprive a person of the right to a fair trial or to an impartial adjudication (5 U.S.C. 552(b)(7)(B)) (reference (a)).

C3.2.1.7.1.3. Could reasonably be expected to constitute an unwarranted invasion of personal privacy of a living person, including surviving family members of an individual identified in such a record (5 U.S.C. 552(b)(7)(C)) (reference (a)).

C3.2.1.7.1.3.1. This exemption also applies when the fact of the existence or nonexistence of a responsive record would itself reveal personally private information, and the public interest in disclosure is not sufficient to outweigh the privacy interest. In this situation, Components shall neither confirm nor deny the existence or nonexistence of the record being requested. This is a Glomar response, and Exemption (7)(C) must be cited in the response. Additionally, in order to insure personal privacy is not violated during referrals, DoD Components shall coordinate with other DoD Components or Federal Agencies **before** referring a record that is exempt under the Glomar concept.

C3.2.1.7.1.3.2. A "refusal to confirm or deny" response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no records" response when a record does not exist and a "refusal to confirm or deny" when a record does exist will itself disclose personally private information.

C3.2.1.7.1.3.3. Refusal to confirm or deny should not be used when 1 the person whose personal privacy is in jeopardy has provided the requester with a waiver of his or her privacy rights; or 2 the person whose personal privacy is in jeopardy is deceased, and the Agency is aware of that fact.

C3.2.1.7.1.3.4. Could reasonably be expected to disclose the identity of a confidential source, including a source within the Department of Defense; a State, local, or foreign agency or authority; or any private institution that furnishes the information on a confidential basis; and could disclose information furnished from a confidential source and obtained by a criminal law enforcement authority in a criminal investigation or by an Agency conducting a lawful national security intelligence investigation (5 U.S.C. 552(b)(7)(D)) (reference (a)).

C3.2.1.7.1.3.5. Would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law (5 U.S.C. 552(b)(7)(E)) (reference (a)).

C3.2.1.7.1.3.6. Could reasonably be expected to endanger the life or physical safety of any individual (5 U.S.C. 552(b)(7)(F)) (reference (a).

C3.2.1.7.2. Some examples of Exemption 7 are:

C3.2.1.7.2.1. Statements of witnesses and other material developed during the course of the investigation and all materials prepared in connection with related Government litigation or adjudicative proceedings.

C3.2.1.7.2.2. The identity of firms or individuals being investigated for alleged irregularities involving contracting with the Department of Defense when no indictment has been obtained nor any civil action filed against them by the United States.

C3.2.1.7.2.3. Information obtained in confidence, expressed or implied, in the course of a criminal investigation by a criminal law enforcement Agency or office within a DoD Component, or a lawful national security intelligence investigation conducted by an authorized Agency or office within a DoD Component. National security intelligence investigations include background security investigations and those investigations conducted for the purpose of obtaining affirmative or counterintelligence information.

C3.2.1.7.3. The right of individual litigants to investigative records currently available by law (such as, the Jencks Act, 18 U.S.C. 3500, (reference (w))) is not diminished.

C3.2.1.7.4. Exclusions. Excluded from the above exemption are the below two situations applicable to the Department of Defense. (Components considering invoking an exclusion should first consult with the Department of Justice, Office of Information and Privacy.)

C3.2.1.7.4.1. Whenever a request is made that involves access to records or information compiled for law enforcement purposes, and the investigation or proceeding involves a possible violation of criminal law where there is reason to believe that the subject of the investigation or proceeding is unaware of its pendency,

and the disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, Components may, during only such times as that circumstance continues, treat the records or information as not subject to the FOIA. In such situation, the response to the requester will state that no records were found.

C3.2.1.7.4.2. Whenever informant records maintained by a criminal law enforcement organization within a DoD Component under the informant's name or personal identifier are requested by a third party using the informant's name or personal identifier, the Component may treat the records as not subject to the FOIA, unless the informant's status as an informant has been officially confirmed. If it is determined that the records are not subject to 5 U.S.C. 552(b)(7) (reference (a)), the response to the requester will state that no records were found.

C3.2.1.8. Number 8. (5 U.S.C. 552 (b)(8)) (reference (a)). Those contained in or related to examination, operation or condition reports prepared by, on behalf of, or for the use of any Agency responsible for the regulation or supervision of financial institutions.

C3.2.1.9. Number 9. (5 U.S.C. 552 (b)(9)) (reference (a)). Those containing geological and geophysical information and data (including maps) concerning wells.

C4. CHAPTER 4

FOR OFFICIAL USE ONLY

C4.1. GENERAL PROVISIONS

C4.1.1. General. Information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from the public *because disclosure would cause a foreseeable harm to an interest protected by* one or more FOIA Exemptions 2 through 9 (see Chapter C3.) shall be considered as being for official use only (FOUO). No other material shall be considered FOUO and FOUO is not authorized as an anemic form of classification to protect national security interests. Additional information on FOUO and other controlled, unclassified information may be found in reference (g) *or by contacting the Directorate for Security, Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence).*

C4.1.2. Prior FOUO Application. The prior application of FOUO markings is not a conclusive basis for withholding a record that is requested under the FOIA. When such a record is requested, the information in it shall be evaluated to determine whether *disclosure would result in a foreseeable harm to an interest protected by one or more FOIA Exemptions 2 through 9. Even* if any exemptions apply, the record *shall* be released as a discretionary matter when it is determined that *there is no foreseeable harm to an interest protected by the exemptions.*

C4.1.3. Historical Papers. Records such as notes, working papers, and drafts retained as historical evidence of DoD Component actions enjoy no special status apart from the exemptions under the FOIA (reference (a)).

C4.1.4. Time to Mark Records. The marking of records at the time of their creation provides notice of FOUO content and facilitates review when a record is requested under the FOIA. Records requested under the FOIA that do not bear such markings shall not be assumed to be releasable without examination for the presence of information that requires continued protection and qualifies as exempt from public release.

C4.1.5. Distribution Statement. Information in a technical document that requires a distribution statement pursuant to DoD Directive 5230.24 (reference (x)) shall bear that statement and may be marked FOUO, as appropriate.

C4.2. MARKINGS

C4.2.1. Location of Markings.

C4.2.1.1. An unclassified document containing FOUO information shall be marked "For Official Use Only" at the bottom on the outside of the front cover (if any), on each page containing FOUO information, and on the outside of the back cover (if any). *Each paragraph containing FOUO information shall be marked as such.*

C4.2.1.2. Within a classified document, an individual page that contains both FOUO and classified information shall be marked at the top and bottom with the highest security classification of information appearing on the page. Individual paragraphs shall be marked at the appropriate classification level, as well as unclassified or FOUO, as appropriate.

C4.2.1.3. Within a classified document, an individual page that contains FOUO information but no classified information shall be marked "For Official Use Only" at the top and bottom of the page, *as well as each paragraph that contains FOUO information.*

C4.2.1.4. Other records, such as photographs, films, tapes, or slides, shall be marked "For Official Use Only" or "FOUO" in a manner that ensures that a recipient or viewer is aware of the status of the information therein.

C4.2.1.5. FOUO material transmitted outside the Department of Defense requires application of an expanded marking to explain the significance of the FOUO marking. This may be accomplished by typing or stamping the following statement on the record prior to transfer:

This document contains information
EXEMPT FROM MANDATORY DISCLOSURE
under the FOIA. Exemption(s) . . . . . applies/apply.

C4.3. DISSEMINATION AND TRANSMISSION

C4.3.1. Release and Transmission Procedures. Until FOUO status is terminated, the release and transmission instructions that follow apply:

C4.3.1.1. FOUO information may be disseminated within DoD Components and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the Department of Defense. Recipients shall be made aware of the status of such information, and transmission shall be by means that preclude unauthorized public disclosure. Transmittal documents shall call attention to the presence of FOUO attachments.

C4.3.1.2. DoD holders of FOUO information are authorized to convey such information to officials in other Departments and Agencies of the Executive and Judicial Branches to fulfill a Government function, except to the extent prohibited by the Privacy Act. Records thus transmitted shall be marked "For Official Use Only," and the recipient shall be advised that the information may qualify for exemption from public disclosure, pursuant to the FOIA, and that special handling instructions do or do not apply.

C4.3.1.3. Release of FOUO information to Members of Congress is governed by DoD Directive 5400.4 (reference (y)). Release to the GAO is governed by DoD Directive 7650.1 (reference (z)). Records released to the Congress or GAO should be reviewed to determine whether the information warrants FOUO status. If not, prior FOUO markings shall be removed or effaced. If withholding criteria are met, the records shall be marked FOUO and the recipient provided an explanation for such exemption and marking. Alternatively, the recipient may be requested, without marking the record, to protect against its public disclosure for reasons that are explained.

C4.3.2. Transporting FOUO Information. Records containing FOUO information shall be transported in a manner that prevents disclosure of the contents. When not commingled with classified information, FOUO information may be sent via first-class mail or parcel post. Bulky shipments, such as distributions of FOUO Directives or testing materials, that otherwise qualify under postal regulations, may be sent by fourth-class mail.

C4.3.3. Electronically and Facsimile Transmitted Messages. Each part of electronically and facsimile transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation "FOUO" before the beginning of the text. Such messages and facsimiles shall be transmitted in accordance with communications security procedures whenever practicable.

C4.4. SAFEGUARDING FOUO INFORMATION

C4.4.1. During Duty Hours. During normal working hours, records determined to be FOUO shall be placed in an out-of-sight location if the work area is accessible to non-government personnel.

C4.4.2. During Nonduty Hours. At the close of business, FOUO records shall be stored so as to prevent unauthorized access. Filing such material with other unclassified records in unlocked files or desks, etc., is adequate when normal U.S. Government or Government-contractor internal building security is provided during nonduty hours. When such internal security control is not exercised, locked buildings or rooms normally provide adequate after-hours protection. If such protection is not considered adequate, FOUO material shall be stored in locked receptacles such as file cabinets, desks, or bookcases. FOUO records that are subject to the provisions of the National Security Act of 1959 (reference (aa)) shall meet the safeguards outlined for that group of records.

C4.5. TERMINATION, DISPOSAL AND UNAUTHORIZED DISCLOSURES

C4.5.1. Termination. The originator or other competent authority; e.g., initial denial and appellate authorities, shall terminate "For Official Use Only" markings or status when circumstances indicate that the information no longer requires protection from public disclosure. When FOUO status is terminated, all known holders shall be notified, to the extent practical. Upon notification, holders shall efface or remove the "For Official Use Only" markings, but records in file or storage need not be retrieved solely for that purpose.

C4.5.2. Disposal.

C4.5.2.1. Nonrecord copies of FOUO materials may be destroyed by tearing each copy into pieces to prevent reconstructing, and placing them in regular trash containers. When local circumstances or experience indicates that this destruction method is not sufficiently protective of FOUO information, local authorities may direct other methods but must give due consideration to the additional expense balanced against the degree of sensitivity of the type of FOUO information contained in the records.

C4.5.2.2. Record copies of FOUO documents shall be disposed of in

accordance with the disposal standards established under 44 U.S.C. 3301-3314 (reference (ab)), as implemented by DoD Component instructions concerning records disposal.

C4.5.3. Unauthorized Disclosure. The unauthorized disclosure of FOUO records does not constitute an unauthorized disclosure of DoD information classified for security purposes. Appropriate administrative action shall be taken, however, to fix responsibility for unauthorized disclosure whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act (reference (d)) may also result in civil and criminal sanctions against responsible persons. The DoD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

1. TITLE	2. IDENTIFICATION NUMBER
OPERATIONS SECURITY (OPSEC) PLAN	DI-MGMT-80934

3. DESCRIPTION / PURPOSE

3.1 The OPSEC Plan describes the methods to: (1) Identify OPSEC security responsibilities and requirements, (2) Define overall OPSEC security standard practice procedures, (3) Identify potential problem areas and determine solutions, and (4) Develop OPSEC security awareness inputs into the overall system security process.

3.2 The Plan is utilized to identify and monitor a contractor's OPSEC activities during performance of the contract.

4. APPROVAL DATE *(YYMMDD)*	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
	NAWCAD 7.4.3		

7. APPLICATION / INTERRALATIONSHIP

7.1 This DID contains the format and content preparation instructions for the data product generated by the specific and discrete task requirements delineated in the contract.
7.2 The DID is applicable only when the contracting activity determines that the sensitivity of the contract warrants the effort.
7.3 The initial submission may be broad in scope; however, the level of detail increases as the work progresses to the point that any security-related question will be addressed in the Plan.
7.4 The contractor's implementation of the OPSEC Plan, approved by the contracting agency, is also subject to joint inspection by the Defense Security Service and the contracting agency.

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER

10. PREPARATION INSTRUCTIONS

10.1 REFERENCE DOCUMENTS: The applicable issue of the document cited herein, including their approval dates and dates of any applicable amendments, notices and revisions shall be as specified in the contract.
10.2 FORMAT: The OPSEC Plan format shall be contractor selected. Unless effective presentation would be degraded the initially used format arrangement shall be used for all subsequent submissions.
10.3 CONTENT: The OPSEC Plan shall include the results of the five-step OPSEC analysis described therein including those applicable to the specific contract.
10.3.1 GENERAL: The OPSEC Plan shall contain details of the OPSEC management concept to include contract identification, assignment of responsibilities, definition of milestones with target dates, provisions for continuous analysis, and periodic revision as the contract activities evolve and become more specific and detailed.
10.3.2 THREAT: The OPSEC Plan shall contain the threat provided by the contracting activity applicable to the specific contract activities.
10.3.3 SENSITIVE ASPECTS OF THE CONTRACT: The OPSEC Plan shall contain an overview of all activities, operations, tests, etc. to be undertaken in the performance of the contract; identify those in which classified information will manifest itself; identify the topics of the classification guide that specify the information is classified; determine how, where, and when the classified information is embodied in the hardware, software, or operations; determine what type access (visual, physical, possession, etc.) permits knowledge of the classified information, what, tools/equipment/capability are required, and the specific national defense advantage provided by the information if it is protected. Based on the above analysis, an Essential Elements of Friendly Information (EEFI) List shall be prepared. This list is to include all the information considered "essential" to the success of the effort, all the information that must be protected to preserve the military advantage potentially provided by the effort. Additionally, the list shall include all the activities, operations, tests, etc. that could reveal the "essential" information to foreign intelligence services (FIS).
10.3.4 VULNERABILITIES: The OPSEC Plan shall contain vulnerabilities derived by comparing threat to sensitive activities to determine which sensitive activities can be observed by FIS. "Observe" is defined to include all physical and chemical properties that can be noted and recorded by any type of sensor to include TEMPEST concerns.The instructions in the Industrial OPSEC Guide shall be followed to identify potential TEMPEST vulnerabilities.
10.3.5 COUNTERMEASURES: The OPSEC Plan shall include the protective measure deemed appropriate for each vulnerability.

11. DISTRIBUTION STATEMENT

DISTRIBUTION STATEMENT B.

CONTRACT DATA REQUIREMENTS LIST
(1 Data Item)

Form Approved
OMB No. 0704-0188

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY: TDP ____ TM- ____ OTHER S (SECURITY)
D. SYSTEM/ITEM	E. CONTRACT / PR NO.	F. CONTRACTOR

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE	17. PRICE GROUP
	OPERATIONS SECURITY (OPSEC) PLAN		18. ESTIMATED TOTAL PRICE

4. AUTHORITY (Data Acquisition document No.)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE
DI-MGMT-80934		NAWCAD 7.4.3

7. DD 250 REQ.	9. DIST STATEMENT REQUIRED	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
8. APP CODE	B	11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION

16. REMARKS

Block 4: Delete references in DI-MGMT-80934. Instead use the definition of sensitive information given in Public Law 100-235; use National Security Directive (NSDD) 298 for the concept of Operations Security.

Block 9: Apply and use distribution statements in accordance with the Distribution Statement Attachment to this contract. See SECNAVINST 5510.36, Chapter 8 for guidance.

Blocks 11, 12 & 13: Preliminary draft plan due 90 days DAC. Final due 45 days after government approval of draft. Revisions are required after approval of final plan only to comply with Government Data Protection Policy Documents revision.

14. DISTRIBUTION

a. ADDRESSEE	b. COPIES Draft	Final Reg	Final Repro
74300ÔA	1	1	0
15. TOTAL →	1	1	0

G. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE

DRAFT ONLY

OPERATIONS SECURITY (OPSEC) PLAN

FOR THE

(PROGRAM/PROJECT)

CONTRACT NO. xxxxxxxxxxxx

CDRL REFERENCE NO. XXXX

DATE:

SUBMITTED TO:

PREPARED BY:

DISTRIBUTION STATEMENT

FOR OFFICIAL USE ONLY

DRAFT ONLY

TABLE OF CONTENTS

DRAFT ONLY

Operations Security Plan

1.0 Purpose

(Usually to establish an OPSEC program for the organization and to direct its implementation.)

2.0 Policy

(State the policy of the organization with regard to protection of information)

3.0 Scope

(What the program includes, i.e., classified and unclassified programs; list exceptions, if any.)

4.0 Background

(Program description and parties involved, i.e., NAWCAD PAX, prime contractor, subcontractors)

5.0 Responsibilities

(OPSEC is the responsibility of everyone assigned to the program. Who is responsible for the overall OPSEC program and who will be responsible for implementation and monitoring of all aspects including revisions and training.)

6.0 Operations Security (OPSEC)

(Basic OPSEC philosophy and approach)

What is OPSEC?

OPSEC is a systematic and proved process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities. The OPSEC process is most effective when fully integrated into all planning and operational processes. The OPSEC process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate countermeasures.

Generally unclassified evidence of the planning and execution of sensitive Government activities could include otherwise unprotected engineer and computer science networking; technology development; technology application(s); and RDT&E thrusts. Other sensitive information that could provide adversaries with insight to critical secrets could include such events as part ordering; prime and subcontractor communications; test and evaluation; and shipping of deliverables. OPSEC usually is concerned with those necessary peripheral actions and events that must occur, but which may also provide a tip-off to the adversary. OPSEC applications rarely affect what occurs, but does affect how things occur, and can be of enormous help in the planning process. OPSEC does not evaluate the effectiveness of traditional security countermeasures. Rather, it assumes that such measures are in place and effective, and concentrates on what is unprotected by those measures.

6.1 Critical Information

(Critical Information is information about friendly intentions, capabilities, or activities that must be protected from loss to keep an adversary from gaining a significant military, economic, political, or technological advantage. The process begins with an examination of the totality of an activity to determine what exploitable but unclassified evidence of classified or sensitive activity is vulnerable to adversary

acquisition in light of the known collection capabilities of potential adversaries. Such evidence is usually derived from openly available data. Certain indicators may be pieced together or interpreted to discern critical information. Indicators commonly stem from the routine administrative, physical, or technical actions taken to prepare for or execute a plan or activity. This section should include, but also expand upon, the data provided by the government sponsor. It should include critical information relating to such things as manufacturing processes or proprietary data or operations that could allow an adversary necessary data to acquire the critical information specified by the government sponsor.)

6.2 Threat

(The plan should contain the threat information provided by the government and any other pertinent information known to the program or activity officials specifying known threat to their location, personnel, information, or operations. Threat should be tailored to both the information and locations identified as critical to the sponsor and the program or activity. An essential part of this section should be a thorough analysis of the available open-source information concerning both the program/activity's and sponsor's operations in similar efforts and technologies. The threat to U.S. Government activities continues. The political changes that took place in eastern Europe have certainly changed the focus of U.S. concerns from a nuclear-centered threat to an economic-centered threat, but the potential for grave harm to the U.S. continues. Although it is a less cataclysmic climate, the ultimate result is the same. Information about specific adversary capabilities is available from the NAWCAD OPSEC Officer. This includes, but not limited to, information on organizations such as the Russian Foreign Intelligence Service (SVRR); People's Republic of China (PRC); Intelligence services of countries friendly to U.S. interests; competitors in the economic world; or efforts by narcotraffickers or terrorist groups.)

6.3 Vulnerabilities

(OPSEC vulnerabilities are normally found in the processes and procedures routinely used by organizations. This section should discuss the process by which vulnerabilities to critical information will be determined. This section will become more focused as the program/activity matures. This part of the plan will require periodic updating based on new threat information and changes in the scope of the program/activity. Determining vulnerabilities involves a systematic analysis of how an operation or activity is actually conducted by the primary and supporting organizations. The organization and activity must be viewed as an adversary might view it. Actions and things that can be observed, or other data that can be interpreted or pieced together to drive critical information, must be identified. These potential vulnerabilities must be matched with specific threats. Once you determine what an adversary needs to know and where that information is available, it is necessary to determine if it is possible that the adversary could acquire and exploit the information in time to capitalize on it . If so, a vulnerability exists.)

6.4 Risk Assessment

(This section should document the requirement for and the process of evaluating the threats to and vulnerabilities of the program/activity. It should be remembered that the purpose of risk assessment is to give an educated opinion or calculation on the probability of critical information loss and its impact, as a guide in taking action. Risk Assessment is essentially the process of balancing a vulnerability against the threat, the deciding if the resultant risk warrants application of countermeasures. The determination of risk is a demanding step in the OPSEC process. It requires a degree of subjective decision making based on the best estimate of an adversary's intentions and capabilities. Included in the assessment of an adversary's capability is not only his ability to collect the information but also his capability to process and exploit (evaluate, analyze, interpret) in time to make use of the information. In order to complete the risk assessment, it is necessary to combine this information (i.e., the possibility of the adversary exploiting the information, with the resultant impact on the organization or program). This process should result in a list of recommendations along with an estimate of the reduced impact upon the operation achieved through their application. The decision maker can then weigh the cost of recommended OPSEC measures in terms of resources and operational effectiveness against the impact of the loss of the critical information.)

6.5 Countermeasures

(For each identified vulnerability, a short list of potential countermeasures should be developed. A detailed assessment of the cost of implementing each countermeasure, the possible impact of not implementing, and appropriate milestones should be provided. Cost should include both direct and indirect monetary impacts. Measures such as cover, counterimagery, and deception may also be recommended. It should be noted, however, that some measures are very costly. A countermeasure is anything that effectively negates an adversary's ability to exploit vulnerabilities. the most effective countermeasures are simple, straightforward, procedural adjustments that effectively eliminate or minimize the generation of indicators. Following a cost-benefit analysis, countermeasures are implemented in priority order to protect vulnerabilities having the most significant impact on the organization, as determined by the appropriate decision maker.

7.0 FOR OFFICIAL USE ONLY/Sensitive Information

FOR OFFICIAL USE ONLY and/or sensitive information control, destruction, transmission, dissemination, storage, and marking requirements must be stated. This information must be secured in a locked office, desk, cabinet, and/or facility. Open storage or unlimited access by individuals at any location is not authorized (normally, corporate proprietary information control procedures a sufficient).

8.0 Public Releases

Any public release of information must be approved by the NAWC OPSEC Officer and the Public Affairs Officer. Public release is, but not limited to, publication of articles in sales medium or media, World Wide Web, symposia, conferences, etc. involving DoD programs/projects or activities.

9.0 Education and Awareness

(Outline how you will educate your employees about OPSEC and this Plan. This training must be accomplished at least once a year. How will you document this training and who is responsible.)

10.0 Point of Contacts

(Who is the focal point in your company for OPSEC (working level))